AMENDMENT TO THE CLAIMS

1. (Currently Amended) A system for automatically updating computer access settings, comprising:

at least one computer access setting for a respective user of a computer, the at least one computer access setting comprising a listing of prohibited computer applications to which access is denied, one version of the at least one computer access setting being stored in a remote database and another version of the at least one computer access setting being stored in the computer; and

a control unit to communicate with the computer and to automatically update the versions of the at least one computer access settings in the computer and the remote database to coincide with each other responsive to at least one computer event, wherein the at least one control access setting being stored in the remote database is updated to reflect changes made to the at least one control access setting being stored in the computer and vice versa, the control unit monitoring a request to launch a computer application that would locally run on the computer's operating system, the control unit intercepting a message for opening a window associated with the requested computer application, the control unit intercepting the message before receipt thereof by the computer's internal operating system to prohibit opening the window, the control unit querying the another version of the computer access settings for the requested computer application, and when the requested computer application is not found in the another version of the computer access settings, then the control unit prohibits opening the window associated with the requested computer application [[,]] to terminate ~~thus terminating~~ the launch of the requested computer application, as the user is not authorized to access the requested computer application.

2. (Original) The system of claim 1, wherein the at least one computer event includes user log-in on the computer and the computer being connected to the Internet.

3. (Original) The system of claim 2, wherein the at least one computer event includes user log-out on the computer and the computer being connected to the Internet.

4. (Original) The system of claim 1, wherein the at least one computer event includes the start up of the computer and the computer being connected to the Internet.

5. (Cancel)

6. (Original) The system of claim 1, wherein the computer access settings contain an allow list of information that the respective user is authorized to access.

7. (Original) The system of claim 1, wherein the computer access settings contain a block list of information that the respective user is not authorized to access.

8. (Original) The system of claim 1, wherein the computer access settings specify if the respective user is authorized to access a particular computer application.

9. (Original) The system of claim 1, wherein the computer access settings specify if the respective user is authorized to access a particular web site.

10. (Original) The system of claim 1, wherein the computer access settings specify if the respective user is authorized to access a category of information that includes computer applications and web sites.

11. (Currently Amended) A system to automatically update computer access information, comprising:

means for creating computer access settings for a respective user of a computer, the computer access settings comprising a listing of prohibited computer applications to which access is denied;

means for storing a first version of the computer access settings in a remote location, the computer access settings comprising a list of restricted computer applications;

means for locally storing a second version of the computer access settings;

means for modifying the first version of the computer access settings; and

means for retrieving the first version of the computer access settings and updating the second version of the computer access settings to coincide with the first version of the computer access settings upon at least one computer event, wherein the first version of computer access settings being stored in the remote location is updated to reflect changes made to the second version of computer access settings being stored locally in the computer and vice versa;

means for monitoring a request to launch a computer application that would locally run on a computer operating system;

means for intercepting a message for opening a window associated with the requested computer application before receipt thereof by the computer's internal operating system to prohibit opening the window;

means for querying the second version of the computer access settings for the requested computer application; and

when the requested computer application is found in the second version of the computer access settings, then means for prohibiting opening the window associated with the requested computer application [[,]] to terminate ~~thus terminating~~ the launch of the requested computer application, as the user is not authorized to access the requested computer application.

12. (Previously Presented) The system of claim 11, wherein the second version of the computer access settings contain a history of user computer activity, the system further comprising:

means for transferring the second version of the computer access settings to the remote location so that the first version at the remote location is updated to include the

history of user computer activity contained in the second version upon the at least one computer event.

13. (Original) The system of claim 11, wherein the at least one computer event includes user log-in on the computer and the computer being connected to the Internet.

14. (Original) The system of claim 12, wherein the at least one computer event includes user log-out on the computer and the computer being connected to the Internet.

15. (Original) The system of claim 11, wherein the at least one computer event includes the start up of the computer and the computer being connected to the Internet.

16. (Original) The system of claim 11, wherein the one version of the computer access settings being stored in the remote database maintains the current authorization settings and the another version of the computer access settings being stored in the computer maintains the latest reporting information.

17. (Original) The system of claim 11, further comprising:

means for prompting an administrator of the computer to specify an allow list of information that the respective user is authorized to access.

18. (Original) The system of claim 11, further comprising:

means for prompting an administrator of the computer to specify a block list of information that the respective user is not authorized to access.

19. (Original) The system of claim 11, further comprising:

means for prompting an administrator of the computer to specify at least one particular computer application that the respective user is not authorized to access.

20. (Original) The system of claim 11, further comprising:

means for prompting an administrator of the computer to specify at least one particular web site that the user respective user is not authorized to access.

21. (Original) The system of claim 11, further comprising:

means for prompting an administrator of the computer to specify at least on particular category of information that the respective user is not authorized to access.

22. (Currently Amended) A method to automatically update computer access information, comprising:

creating computer access settings for a respective user of a computer, the computer access settings comprising a listing of prohibited computer applications to which access is denied;

storing a first version of the computer access settings in a remote location;

locally storing a second version of the computer access settings;

modifying the first version of the computer access settings;

upon at least one computer event, retrieving the first version of the computer access settings and updating the second version of the computer access settings to coincide with the first version of the computer access settings, wherein the first version of computer access settings being stored in the remote location is updated to reflect changes made to the second version of computer access settings being stored locally in the computer and vice versa;

monitoring a request to launch a computer application that would locally run on a computer operating system;

intercepting a message for opening a window associated with the requested computer application before receipt thereof by the computer's internal operating system to prohibit opening the window;

querying the second version of the computer access settings for the requested computer application; and

prohibiting opening the window associated with the requested computer application when the requested computer application is found in the second version of the computer access settings [[,]] to terminate ~~thus terminating~~ the launch of the requested computer application, as the user is not authorized to access the requested computer application.

23. (Cancel)

24. (Original) The method of claim 22, wherein the at least one computer event includes user log-in on the computer and the computer being connected to the Internet.

25. (Original) The method of claim 23, wherein the at least one computer event includes user log-out on the computer and the computer being connected to the Internet.

26. (Original) The method of claim 22, wherein the at least one computer event includes the start up of the computer and the computer being connected to the Internet.

27. (Previously Presented) The method of claim 22, wherein the first version of the computer access settings being stored in the remote database maintains the current authorization settings and the second version of the computer access settings being stored in the computer maintains the latest reporting information.

28. (Previously Presented) The method of claim 22, further comprising:

prompting an administrator of the computer to specify an allow list of information that the respective user is authorized to access.

29. (Previously Presented) The method of claim 22, further comprising:

prompting an administrator of the computer to specify a block list of information that the respective user is not authorized to access.

30. (Previously Presented) The method of claim 22, further comprising:

prompting an administrator of the computer to specify at least one particular computer application that the respective user is not authorized to access.

31. (Previously Presented) The method of claim 22, further comprising:

prompting an administrator of the computer to specify at least one particular web site that the user respective user is not authorized to access.

32. (Previously Presented) The method of claim 23, further comprising:

prompting an administrator of the computer to specify at least on particular category of information that the respective user is not authorized to access.

33. (Currently Amended) A computer-readable memory storing processor executable instructions for performing a method that controls computer access to Internet content, the method comprising:

creating computer access settings for a respective user of a computer, the computer access settings comprising a listing of prohibited computer applications to which access is denied and time restrictions that the user is not authorized to access a computer;

storing a first version of the computer access settings in a remote location;

locally storing a second version of the computer access settings;

modifying the first version of the computer access settings;

upon at least one computer event, retrieving the first version of the computer access settings and updating the second version of the computer access settings to coincide with the first version of the computer access settings, wherein the first version of computer access settings being stored in the remote location is updated to reflect changes made to the second version of computer access settings being stored locally in the computer and vice versa;

querying a remotely located server for a current time;

preventing manipulation of a local clock setting by preferring the current time obtained from the remote server;

comparing the current time to the time restrictions;

monitoring a request to launch a computer application that would locally run on a computer operating system;

intercepting a message for opening a window associated with the requested computer application before receipt thereof by the computer's internal operating system to prohibit opening the window;

querying the second version of the computer access settings for the requested computer application;

prohibiting opening the window associated with the requested computer application when the requested computer application is found in the second version of the computer access settings [[,]] to terminate ~~thus terminating~~ the launch of the requested computer application, as the user is not authorized to access the requested computer application.

34. (Cancel)

35. (Previously Presented) The computer readable memory of claim 33, wherein the at least one computer event includes user log-in on the computer and the computer being connected to the Internet.

36. (Previously Presented) The computer readable memory of claim 34, wherein the at least one computer event includes user log-out on the computer and the computer being connected to the Internet.

37. (Previously Presented) The computer readable memory of claim 33, wherein the at least one computer event includes the start up of the computer and the computer being connected to the Internet.

38. (Previously Presented) The computer readable memory of claim 33, wherein the one version of the computer access settings being stored in the remote database maintains the current authorization settings and the another version of the computer access settings being stored in the computer maintains the latest reporting information.

39. (Previously Presented) The computer readable memory of claim 33, the program further comprising:

prompting an administrator of the computer to specify an allow list of information that the respective user is authorized to access.

40. (Previously Presented) The computer readable memory of claim 33, the program further comprising:

prompting an administrator of the computer to specify a block list of information that the respective user is not authorized to access.

41. (Previously Presented) The computer readable memory of claim 33, the program further comprising:

prompting an administrator of the computer to specify at least one particular computer application that the respective user is not authorized to access.

42. (Previously Presented) The computer readable memory of claim 33, the program further comprising:

prompting an administrator of the computer to specify at least one particular web site that the user respective user is not authorized to access.

43. (Previously Presented) The computer readable memory of claim 34, the program further comprising:

prompting an administrator of the computer to specify at least on particular category of information that the respective user is not authorized to access.